



Ejercicio 2: Clasificación y Ética de Ciberatacantes

Ejercicio Práctico: Exploración de OWASP Juice Shop y ataques básicos de login

Objetivo general: Comprender los distintos tipos de ciberatacantes a través de un laboratorio práctico que simula ataques reales contra un entorno vulnerable. Este ejercicio también refuerza los principios éticos del hacking responsable.

Parte 1: Implementación del entorno vulnerable

Para comenzar este ejercicio, debes desplegar una instancia funcional del entorno OWASP Juice Shop utilizando Docker Compose.

Crea un archivo llamado `docker-compose.yml` con el siguiente contenido:

```
version: "3.8"
```

```
services:
```

```
  juice-shop:
```

```
    image: bkimminich/juice-shop
```

```
    container_name: juice-shop
```

```
    ports:
```

```
      - "3000:3000"
```

```
    restart: unless-stopped
```


Guarda el archivo y, desde la terminal, ejecuta:

```
docker-compose up -d
```

Esto iniciará el entorno vulnerable. Accede al sistema desde tu navegador en:

```
http://localhost:3000
```

Parte 2: Acceso por credenciales por defecto

 **Objetivo:** Entrar al sistema usando credenciales conocidas o débiles, una práctica común entre atacantes *Black Hat*.


1. Haz clic en el ícono de usuario (esquina superior derecha) y selecciona **"Login"**.
2. Prueba los siguientes datos de acceso:

Email: admin@juice-sh.op
Password: admin123


O alternativamente:

Email: jim@juice-sh.op
Password: ncc-1701

3. Si lograste acceder, observarás que aparece el nombre del usuario en la esquina. Esto confirma que el sistema **no tiene mecanismos de protección contra contraseñas por defecto**.

 **Reflexión:** Este tipo de acceso sería una técnica típica de un **hacker de sombrero negro**. El mismo conocimiento, en manos de un **hacker ético**, permite reportar y corregir estas fallas.

Parte 3: Prueba de inyección SQL en el login

 **Objetivo:** Realizar un ataque de inyección SQL básico para evadir el proceso de autenticación.

Vuelve al formulario de login y prueba los siguientes datos:

Email: ' OR 1=1--
Password: cualquiercosa

O bien:

Email: ' OR '1'='1
Password: anything

Si logras ingresar sin un usuario válido, habrás explotado una vulnerabilidad crítica de **inyección SQL**, lo que demuestra la ausencia de validaciones en el backend del aplicativo.

Reflexión final

Este laboratorio muestra cómo los conocimientos técnicos pueden ser utilizados de forma **constructiva o destructiva**, dependiendo de la ética del atacante. Reflexiona sobre estas preguntas:

- ¿Qué tipo de hacker sería capaz de explotar estas fallas con intención maliciosa?
 - ¿Cómo actuaría un hacker ético frente a este descubrimiento?
 - ¿Qué medidas debería tomar la organización para evitar estos accesos?
-